Z. Noor Fatima* et al.
(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.4, Issue No.5, August – September 2016, 3573 – 3575.

# Deploying An Unique Control Scheme To Reduce The Identity Leakage

**Z.NOOR FATIMA**
M.Tech Student, Dept of CSE
Malla Reddy Engineering College for Women
Hyderabad, T.S, India

**B.V.S.P.PAVAN KUMAR**
Associate Professor, Dept of CSE
Malla Reddy Engineering College for Women
Hyderabad, T.S, India

*Abstract:* **The help of cloud computing has attracted much attention from academia in addition to industry due to profitability however it's several challenges. Within our work we advise a competent way of enabling cloud servers to manage user access rights lacking of knowing their identity data. The suggested product is a semi-anonymous privilege control proposal for controlling of not just data privacy, but furthermore user identity privacy within traditional techniques of access control. This method decentralizes central authority to limit the leakage of identity and therefore attains semi-anonymity. Additionally, it furthermore generalizes file access control for privilege control, through which rights from the entire procedures over the system of cloud data re handled within fine-grained manner.**

*Keywords:* **Cloud Computing; Fine Grained; Semi-Anonymous; Data Privacy; Central Authority; Privileges;**

## I. INTRODUCTION

Many techniques were suggested to help keep data contents privacy through access control. Identity-based file encryption was introduced in which the message sender specifies a name to ensure that only receiver by way of matching identity decrypts it. Later the fuzzy Identity-based file encryption was suggested, referred to as Attribute-Based File encryption. And then many tree-based techniques of Attribute-Based File encryption, Key-Policy based file encryption and cipher text-policy based file encryption were brought to condition more general form than easy overlap. Within the Key-Policy based file encryption a cipher-text is related using a group of characteristics, and secret is connected with a monotonic access structure much like a tree, which describes user identity [1]. Within the cipher text-policy based file encryption, cipher-texts are created by way of an access structure, which identify file encryption policy, and generate private keys with regards to users' characteristics. Not the same as data privacy, fewer efforts are compensated for safeguarding privacy of user identity during interactive methods. User identity that is described by way of their characteristics is revealed towards key companies, and companies will issue private keys with regards to their characteristics. Nevertheless it appears normal that customers want to maintain their identity secret when they still acquire their private keys. Hence within our work we advise AnonyControl for enabling cloud servers to manage user access rights lacking of knowing their identity data. The suggested product is a semi-anonymous privilege control proposal for controlling of not just data privacy, but furthermore user identity privacy within traditional techniques of access control. Suggested plan is semi-anonymous as partial identity details are revealed to each one of the authority, but we are able to achieve full-anonymity and furthermore permit collusion of government bodies. The suggested method decentralizes central authority to limit the leakage of identity and therefore attains semi-anonymity. Besides, it furthermore generalizes file access control for privilege control, through which rights from the entire procedures over the system of cloud data re handled within fine-grained manner.

## II. METHODOLOGY

Cloud computing technology gives flexible, economical utilization of computing sources. However the information is outsourced towards a few of the cloud servers, and a number of privacy concerns emerge from this. We've got the technology of cloud computing has attracted much attention from academia in addition to industry due to profitability nevertheless it furthermore has three challenges that needs to be handled. First of all, data confidentiality should be assured [2]. The information privacy isn't just concerning data contents. As the best looking a part of cloud computing is computation outsourcing, it's far enough to simply execute an access control. Next, private data reaches risk as one's identity is reputable according to his data for aim of access control. While individuals are more concerned regarding identity privacy, the identity privacy furthermore must be handled before cloud entering our existence. Finally cloud computing system needs to be resilient within the situation of security breach where some a part of product is compromised by way of attackers. We advise semi-anonymous privilege control proposal for enabling cloud servers to manage user access rights lacking of knowing their identity data. The suggested product is for controlling of not just data privacy, but furthermore user identity privacy within

  

traditional techniques of access controls [3]. This process decentralizes central authority to limit the leakage of identity and therefore attains semi-anonymity and furthermore generalizes file access control for privilege control, through which rights from the entire procedures over the system of cloud data re handled within fine-grained manner. Within our plan, numerous trees are essential in every computer file to verify user identity and also to grant him advantage. The suggested schemes safeguard user privacy against each one of the single authority. Partial details are revealed inside the suggested system and also the plan is tolerant against authority compromise.

## III. AN OVERVIEW OF PROPOSED SYSTEM

Within our suggested system, you will find four organizations for example attribute government bodies, cloud server, data proprietors in addition to data consumers. A person may well be a data owner in addition to a data consumer simultaneously. Government bodies are assumed to contain influential computation capabilities, and they're handled by way of government offices as some characteristics partially contain user identifiable data. The entire attribute set is separated as N disjoint sets and handled by each one of the authority, thus each authority is mindful of only element of characteristics. Data owner is entity who outsources encoded computer file towards cloud servers. Cloud Server should really contain enough storage capacity. Recently became a member of consumers of information request private keys from entire government bodies, and they don't write out which characteristics are handled through which government bodies. When consumers of information create a request of the private keys from government bodies, government bodies mutually make equivalent private key and forward it for them. The whole data consumers download encoded documents only that private keys which assure privilege tree can transport out operation that is associated with the privilege [4]. The server is allocated to do a function when and just if user's credentials are verified by way of privilege tree. Cloud has lots of challenges that needs to be handled for example first of all, data confidentiality should be assured next, private data reaches risk as one's identity is reputable according to his data for aim of access control and lastly cloud computing system needs to be resilient within the situation of security breach where some a part of product is compromised by way of attackers. The suggested system permits cloud servers to manage user access rights lacking of knowing their identity data. It manages not just data privacy, but furthermore user identity privacy within traditional techniques of access control and decentralizes central authority to limit the leakage of identity and therefore attains semi-anonymity. Within our work file encryption policy is described using a tree referred to as access tree. Each one of the non-leaf nodes of tree is really a threshold gate, and each one of the leaf nodes is described by way of a characteristic. One access tree is essential in every computer file for determining of file encryption policy. The suggested system generalizes file access control for privilege control, through which rights from the entire procedures over the system of cloud data re handled within fine-grained manner. The privilege within our system is identified as much like rights which are handled in normal os's [5]. Within our system, numerous trees are essential in every computer file to verify user identity and also to grant him benefit accordingly. Within our work we believed semi-honest government bodies within the suggested system and understood that they'll not collude with one another. It is really an essential statement in suggested system since each one of the authority is accountable of the subset of complete characteristics set, as well as for characteristics that it's responsible of also it knows precise information of key requester. Once the data in the entire government bodies is collected as a whole, total attribute group of key requester is enhanced and for that reason his identity is revealed to government bodies. Therefore, the suggested product is semi-anonymous as partial identity details are revealed to each one of the authority, but we are able to achieve full-anonymity and furthermore permit collusion of government bodies.

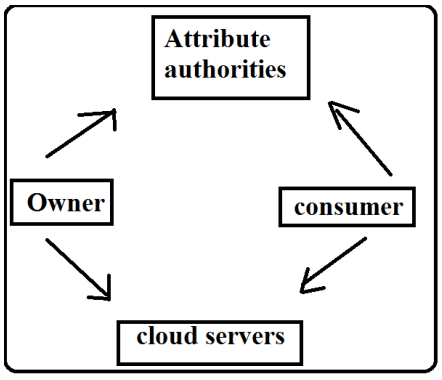


***Fig1: proposed system.***

## IV. CONCLUSION

The majority of the schemes based on attribute-based file encryption were suggested for acquiring of cloud storage. However, the majority of the work concentrates on privacy of information contents and access control, while less consideration is compensated towards privilege control in addition to identity privacy. We recommend a procedure for enabling cloud servers to manage user access rights lacking of knowing their identity data. The suggested strategy is a semi-anonymous privilege control proposal for

  

controlling of not just data privacy, but furthermore user identity privacy within traditional techniques of access control. The process decentralizes central authority to limit the leakage of identity and therefore attains semi-anonymity. It generalizes file access control for privilege control, through which rights from the entire procedures over the system of cloud data re handled within fine-grained manner. The suggested system safeguards user privacy against each one of the single authority. Partial details are revealed inside the suggested system and also the plan is tolerant against authority compromise.

## V. REFERENCES

[1] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," Information Sciences, vol. 180, no. 13, pp. 2618–2632, 2010.

[2] H. Ma, G. Zeng, Z. Wang, and J. Xu, "Fully secure multi-authority attribute-based traitor tracing," JCIS, vol. 9, no. 7, pp. 2793–2800, 2013.

[3] Y. Liu, J. Han, and J. Wang, "Rumor riding: anonymizing unstructured peer-to-peer systems," TPDS, vol. 22, no. 3, pp. 464–475, 2011.

[4] A. Kapadia, P. Tsang, and S. Smith, "Attribute-based publishing with hidden credentials and hidden policies," NDSS, 2007.

[5] L. Zhang, X.-Y. Li, and Y. Liu, "Message in a sealed bottle: Privacy preserving friending in social networks," in ICDCS. IEEE, 2013, pp. 327–336.

  